

[c)]establishing a second stream between the second process and the communication channel;

[d)]in response to the data being written to the first stream, encrypting the data to generate encrypted data, the encrypting of the data being performed independent of any communication protocol layers used to transport the encrypted data from the first network node to the second network node;

[e)]causing the encrypted data to be transmitted from the first network node to the second network node according to the at least one communication protocol layer supported by the first and second network nodes; and

[f)]in response to the encrypted data being read from the second stream, decrypting the encrypted data to recover decrypted data which is identical to the data on the first network node before the data was written to the first stream, the decrypting of the encrypted data being performed independent of any communication protocol layers used to transport the encrypted data from the first network node to the second network node.

*Sub
FS* 2. (TWICE AMENDED) The method of Claim 1, further including the steps of

[a)]performing a communication protocol layer specific encryption of the data on the first network node, and

[b)]performing a communication protocol layer specific decryption of the data on the second network node.

4. (TWICE AMENDED) The method of Claim 1, wherein the communication channel is a Java secure channel, wherein the first stream is a Java stream, wherein the second stream is a Java stream, wherein the method further comprises the step of connecting the Java secure channel to a third Java stream, and wherein the third Java stream provides for the transmission of data according to a specific communication protocol layer.

82

5. (TWICE AMENDED) A computer-readable medium carrying one or more sequences of one or more instructions for providing communication protocol layer independent security for data transmitted between a first process, executing on a first network node, and a second process, executing on a second network node, wherein the first network node and the second network node each support at least one common communication protocol layer, the one or more sequences of one or more instructions including instructions which, when executed by one or more processors, cause the one or more processors to perform the steps of:

- [a]]establishing a communication channel between the first network node and the second network node;
- [b]]establishing a first stream between the first process and the communication channel;
- [c]]establishing a second stream between the second process and the communication channel;

[d] in response to the data being written to the first stream, encrypting the data to generate encrypted data, the encrypting of the data being performed independent of any communication protocol layers used to transport the encrypted data from the first network node to the second network node;

E2
Cont

[e] causing the encrypted data to be transmitted from the first network node to the second network node according to the at least one communication protocol layer supported by the first and second network nodes; and

[f] in response to the encrypted data being read from the second stream, decrypting the encrypted data to recover decrypted data which is identical to the data on the first network node before the data was written to the first stream, the decrypting of the encrypted data being performed independent of any communication protocol layers used to transport the encrypted data from the first network node to the second network node.

6. (TWICE AMENDED) The computer-readable medium of Claim 5, wherein the computer-readable medium further includes instructions for performing the steps of

[a] performing a communication protocol layer specific encryption of the data on the first network node, and

[b] performing a communication protocol layer specific decryption of the data on the second network node.

E3

13. (TWICE AMENDED) A computer data signal embodied in a carrier wave and representing sequences of instruction which, when executed by one or more processors, provide communication protocol layer independent security for data transmitted between

a first process, executing on a first network node, and a second process, executing on a second network node, according to at least one common communication protocol layer supported by the first and second network nodes, by performing the steps of:

- E3
Cont*
- [a] establishing a communication channel between the first network node and the second network node;
 - [b] establishing a first stream between the first process and the communication channel;
 - [c] establishing a second stream between the second process and the communication channel;
 - [d] in response to the data being written to the first stream, encrypting the data to generate encrypted data, the encrypting of the data being performed independent of any communication protocol layers used to transport the encrypted data from the first network node to the second network node;
 - [e] causing the encrypted data to be transmitted from the first network node to the second network node according to the at least one communication protocol layer supported by the first and second network nodes; and
 - [f] in response to the encrypted data being read from the second stream, decrypting the encrypted data to recover decrypted data which is identical to the data on the first network node before the data was written to the first stream, the decrypting of the encrypted data being performed independent of any communication protocol layers used to transport the encrypted data from the first network node to the second network node.

E3
14. (TWICE AMENDED) The computer data signal of Claim 13, wherein the computer sequence of instructions further includes instructions for performing the steps of

[a]]performing a communication protocol layer specific encryption of the data on the first network node, and

[b]]performing a communication protocol layer specific decryption of the data on the second network node.

E4
23. (AMENDED) The method of claim 20, wherein:

the communication channel is a Java secure channel;

the first stream is a Java stream;

the second stream is a Java stream;

the method further comprises the step of connecting the [the] Java secure channel to a third Java stream; and

the third Java stream provides for the transmission of data according to a specific communication protocol layer.

REMARKS

Claims 1-8 and 13-35 are pending in the application. Claims 1-2, 4-6, 13-14, and 23 are amended. For the following reasons, this application should be considered in condition for allowance and the case passed to issue.

The Examiner commented that Figures 1-6 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. The Applicants respectfully